Information Assurance Security Awareness Briefing

After Slide Show starts, click your mouse or press the Page Down key on your keyboard to continue

Note: THIS SLIDE SHOW WAS DONATED TO THE IA COMMUNITY BY:

Strategic Planning & Information

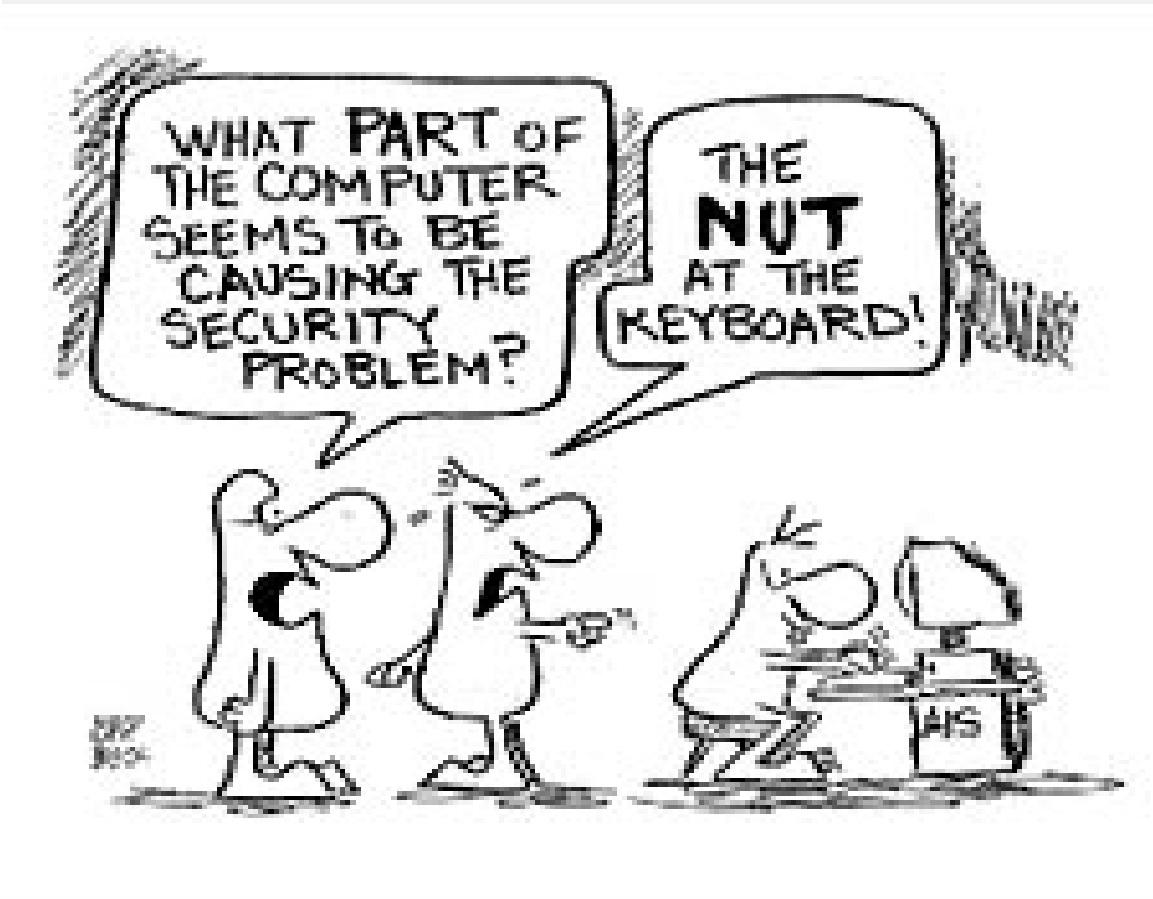
DISA Information Assurance Branch

(SI22)

Overview

- What is Information Assurance
- General Security Guidance
- Protecting Information
- Reporting Violations
- What can you do?

Are you the Problem or the Solution?



What is Information Assurance?

Information Assurance is:

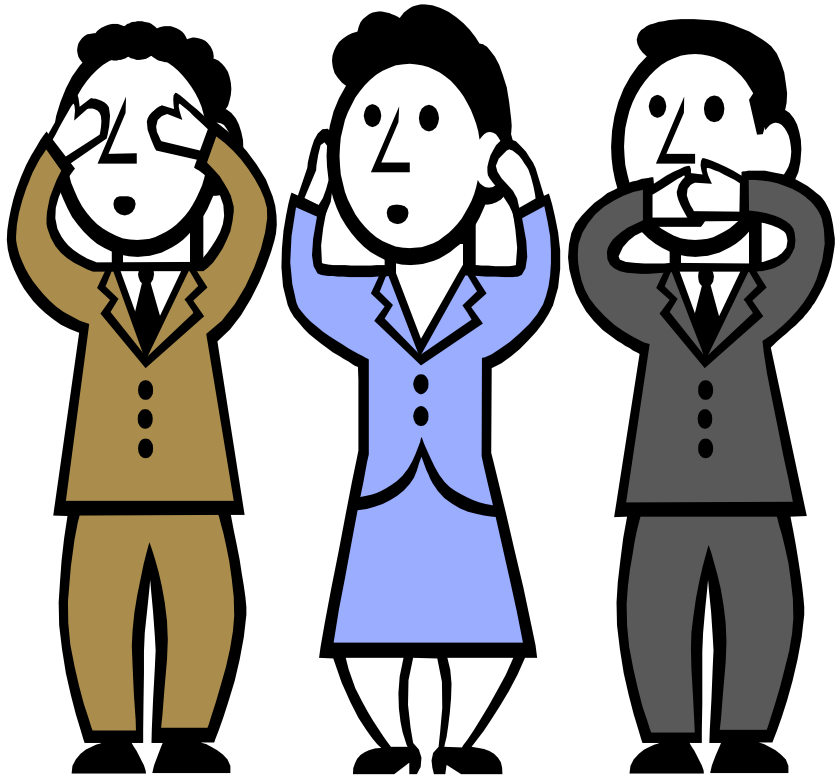
“ Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation…providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.”

as defined by the CNSSI 4009, “ National Information Systems Security Glossary,” dated May 2003

What is Information Assurance?

- Making sure the computer and the information is there when we need it (Availability).
- Making sure the information we use, transmit, process, or stored has not been corrupted or adversely manipulated (Integrity).
- Making sure we know who is using our computers and accessing our data (Authentication).
- Making sure the information is protected from disclosure (Confidentiality).
- Making sure the information is ‘tagged’ so when we send it – we know it got there, and the recipient knows who sent it (Nonrepudiation).

So, Why Are You Here?

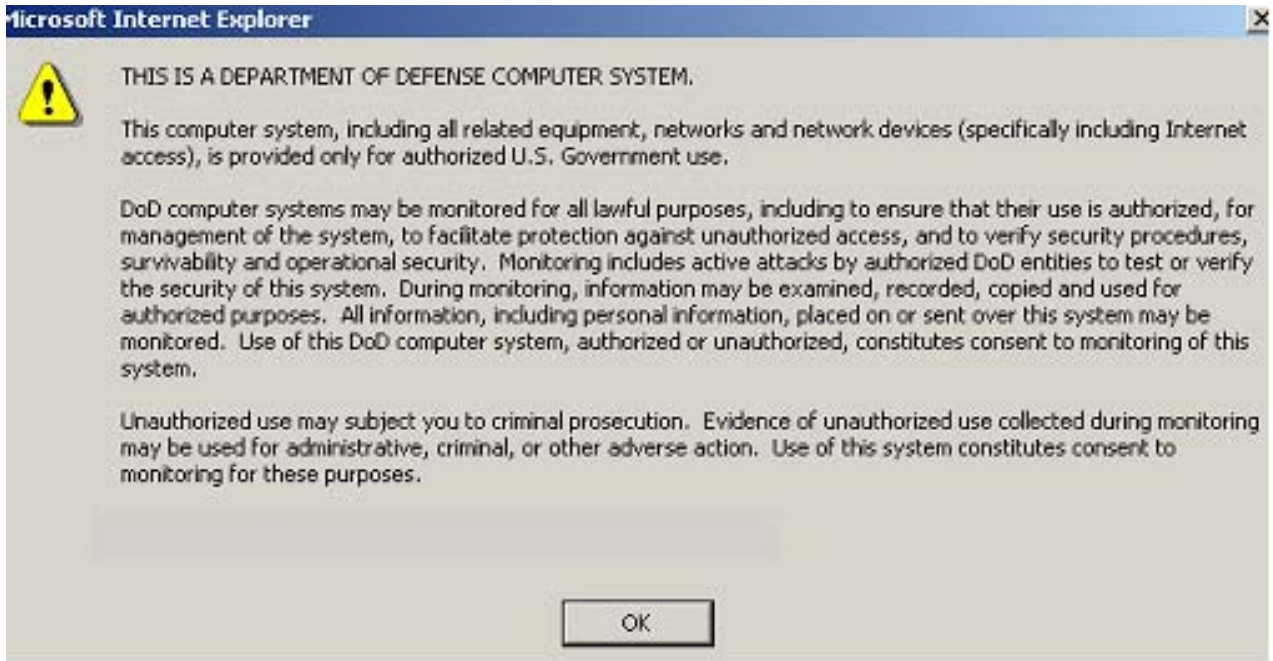


- **DOD policy requires annual information assurance awareness training**
- **Need to emphasize important security tasks and acceptable user practices**

Your Mission…Should you decide to accept it…

- **Recognize your computing responsibilities.**
- **Accept responsibility for protecting government information.**
- **Recognize the challenges and threats that can harm our National Security.**

Do you know what “OK” means?



When you click “OK” :

- **You acknowledge that the information system you use is for “Official Government Use Only.”**
- **Your computer and all of its information are subject to inspection.**
- **Your actions are subject to continuous audit.**

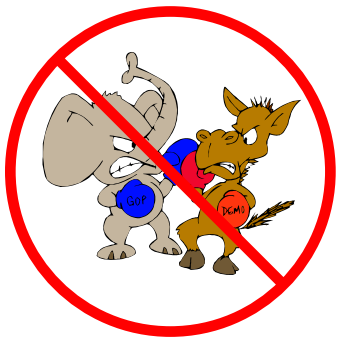
General Workstation Security

- Protect your identity (User Id)
- Use Strong Passwords
  - Make passwords 8 characters or longer
    - use capital letters, numbers, and punctuation symbols
  - Change passwords often
- Always Lock your PC while leaving it unattended
  - Press Control+ALT+Delete and click the “Lock Workstation” Button
- Use your Common Access Card (CAC) to digitally sign and encrypt your sensitive emails
  - Take your CAC with you when you leave your work area

You are responsible for the data on your system at all times!

Prudent Network Security and Internet Practices

- **Email and Internet Use**
  - **Do not open emails from individuals that you do not recognize**
    - **Report suspicious emails to the DISANet Help Desk and your security manager.**
  - **Incidental personal use is permitted.**
- **DISANet prohibits the use of Email or the Internet for:**

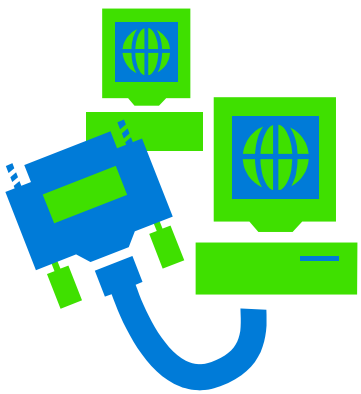


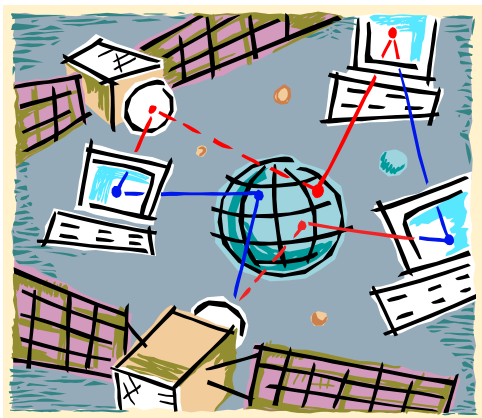
  - **Chain letters**
  - **Private commercial activities**
  - **Accessing pornographic or gambling sites**
  - **Participating in online auction activity**
  - **Political Activity**
  - **Illegal fraudulent or malicious activities**
  - **Any use which reflects adversely on DISA or any other DOD element**
- **Virus Protection**
  - **Avoid attaching media from unfamiliar computing environments.**
  - **Ensure your workstation runs a daily virus scan.**

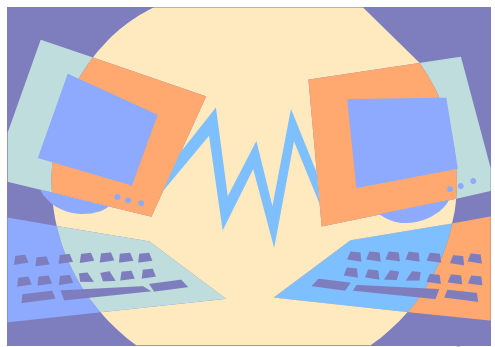
"Trust, but Verify"

What is P2P and What is the Risk?

- Peer-to-Peer file sharing is technology that allows users to typically share music/video files.
- It is risky! It bypasses security or control mechanisms.
- Opens DOD networks to attacks and intrusions!







What are the Dangers of P2P?

- **The default settings of P2P applications share all documents and media files on your machine.**
  - **This causes the potential for disclosure of sensitive information.**

- **P2P applications create open doors that may b remotely exploited to compromise DOD systems.**
- **P2P software puts excessive strain on the network resources.**
  - **This will overwhelm our infrastructure already operating at 90% capacity.**
- **P2P file exchanges generally violate international copyright laws.**

What should I do?

Don't Use it!

- **ASD (NII) Memo, Elimination of Unauthorized Peer-to-Peer File Sharing Applications Across DOD, 13 April 2004.**

- **There are many legal and security issues, and there is no mission essential aspect to P2P applications.**

- **DO NOT USE P2P software on government assets**
  - **Forbidden software includes (but is not limited to):**

Napster **ARES** **IRC Chat Relay**
Kazaa **Limewire** **BitTorrent**
Morpheus **Gnutella**

Got Wireless?

- **DOD Directive 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG),"**
  - **This directive outlines the DOD wireless policy to ensure a secure use of wireless technology throughout the agency.**

Does this Apply to Me?

- This Policy Applies to all
  - DOD Personnel, Contractors, and visitors that have access to DOD Information.
  - All (government owned/used) commercial wireless devices, services and technologies including but not limited to:

- Laptops with WiFi
- Cellular or PCS Devices
- Audio/Video Recorders
- Personal Data Assistants
- Messaging Devices
- Any other wireless device capable of storing, processing, or transmitting information

Exempted are:

– Receive only pagers

– GPS Receivers

– Hearing Aids, Pace makers, other implanted medical devices or personal life support systems

–The Detection Segment of a PED

- The signal between a barcode reader and receiver
- A TV remote and television

– RF Identification Tags (both Active and Passive)

What are my Duties?

Employee Owned Equipment	Government Owned Equipment
• Do not process government information on personally owned laptops, PDAs, or cell phones. • Do not attempt to connect personally owned wireless devices to government networks. • Turn off camera phones and PDAs with camera modules in classified areas.	• Enable Wired Equivalent Privacy (WEP) on all laptops, PDAs and wireless access points. • When computers are plugged into the network, disable any wireless cards. • Enable Encryption on all wireless transmissions • Turn off wireless devices in classified areas.

Never transmit CLASSIFIED data using a wireless device!

What is Information?

- **Information is: Any knowledge that can be communicated regardless of its physical form or characteristic.**

- **Information is classified by the degree of damage which would be caused if the information was revealed.**

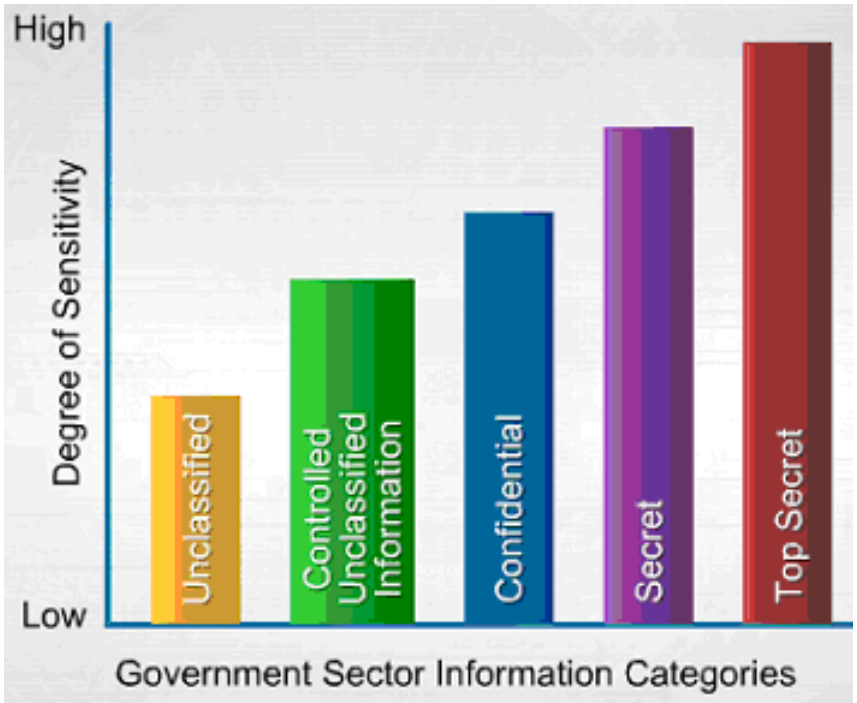
There are 3 levels of classification:

- **TOP SECRET - unauthorized disclosure could cause exceptionally grave damage to national security.**
- **SECRET - unauthorized disclosure could cause serious damage to national security.**
- **CONFIDENTIAL - unauthorized disclosure could cause damage to national security.**

- **Sensitive Compartmented Information (SCI):**
  - **Requires more stringent security protection.**
  - **Protects intelligence sources and methods.**

What is Information? (Con't)

- **"Controlled Unclassified Information" is the DOD term used to define sensitive information such as:**
  - **For Official Use Only (FOUO)**
  - **Contract Sensitive**
  - **Proprietary**

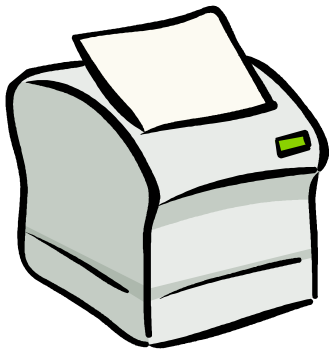


Protection of Computerized Information

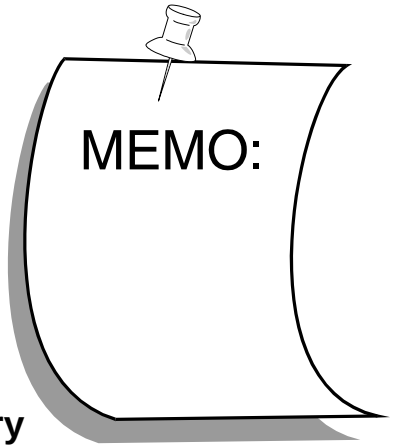
- At Rest
- In Transit
- In Process

Information At Rest

Information can be stored on:

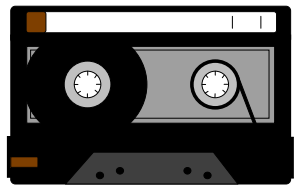


Printers with memory



Printed Documents

CDs or Floppy Disks



Backup Tapes

Fax Machines

Handheld Devices

Computer Hard Drives

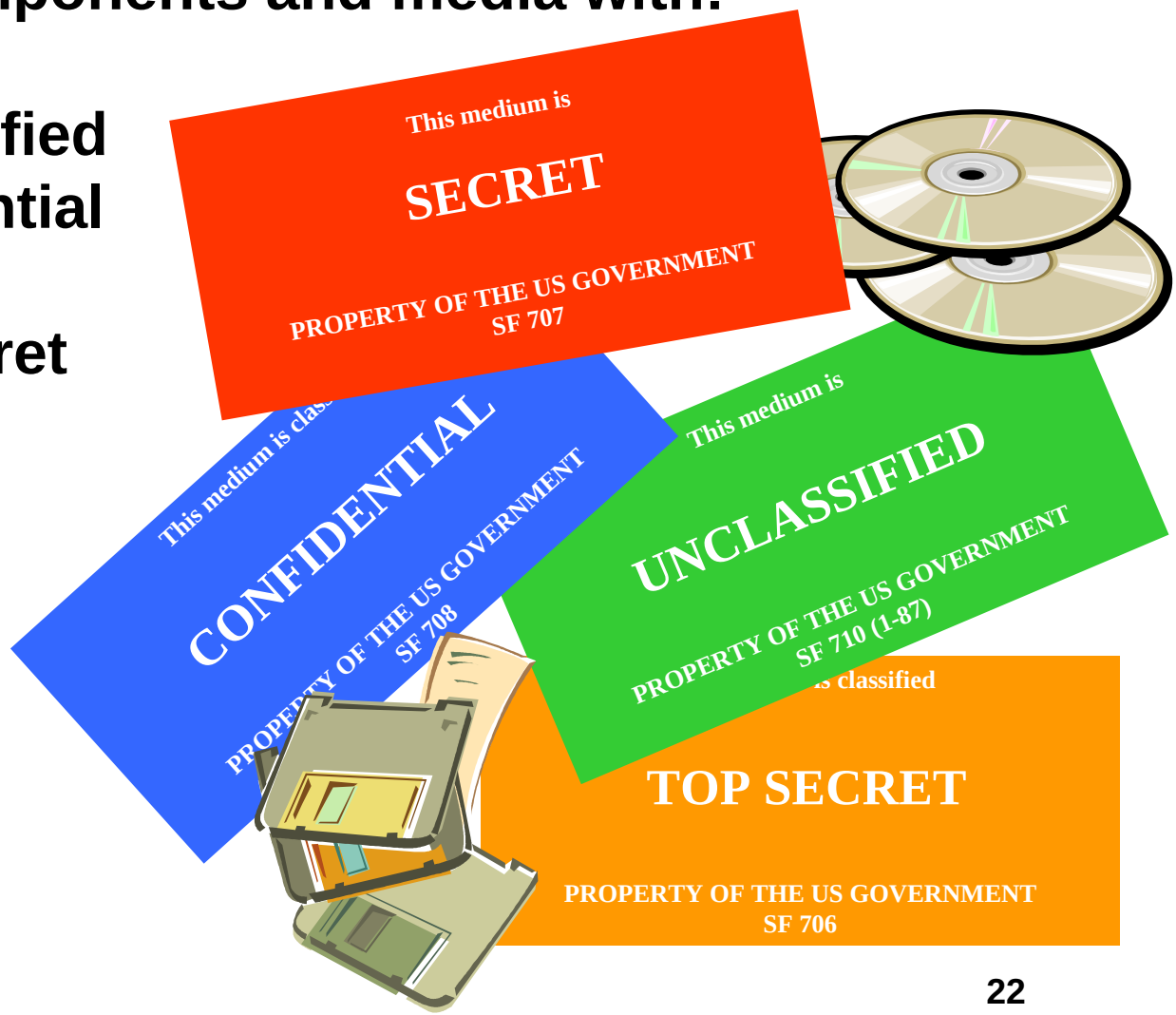
WEB Pages

DOD treats all media as documents.

MARK STORAGE MEDIA

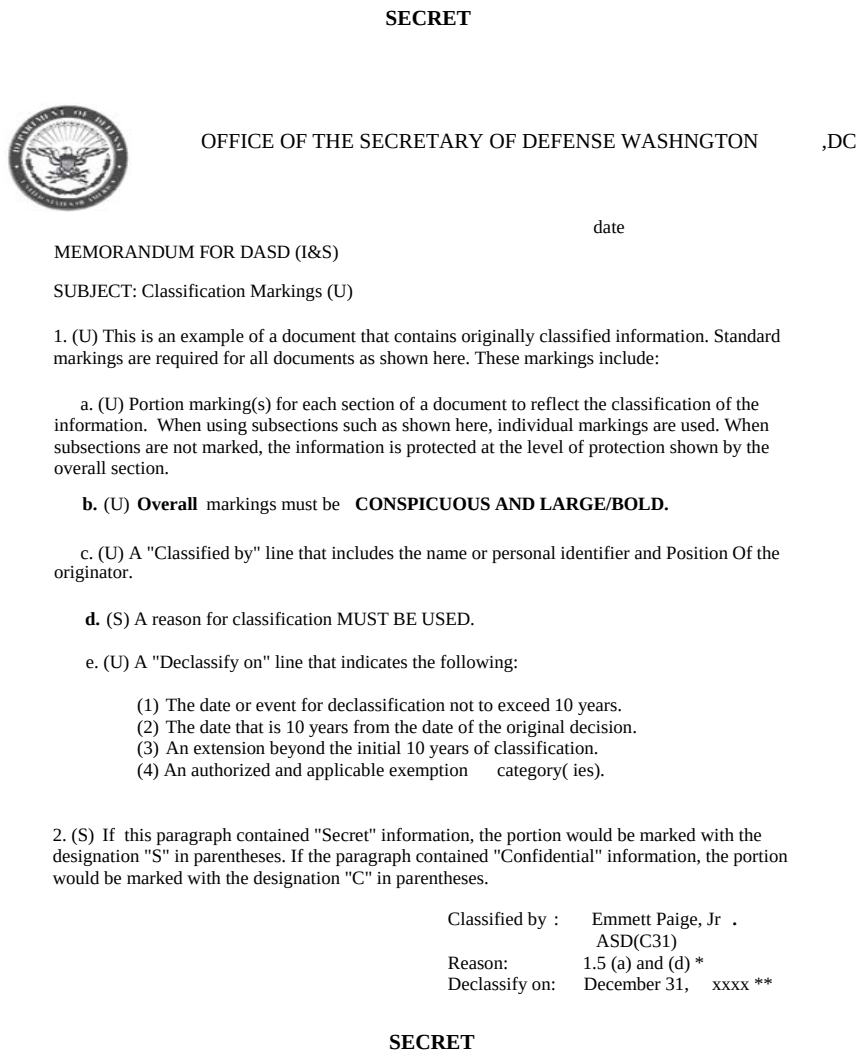
Mark computer components and media with:

- **SF 710 Unclassified**
- **SF 708 - Confidential**
- **SF 707 - Secret**
- **SF 706 - Top Secret**



The Fundamentals of Marking

- **Documents must be marked according to Classification Level or Information Sensitivity.**
- **Markings must be conspicuous!**
  - **Large/Bold lettering**
  - **Use no abbreviations**
- **Classification/sensitivity of documents must "stand out" - either electronically or stamped manually.**
- **Mark top & bottom of each page.**
  - **FOR OFFICIAL USE ONLY (FOUO) is marked on the bottom of page only**
  - **FOUO guidance please visit https://datahouse.disa.mil/gc/fouo.html**
- **Paragraph, portion, and title markings may be abbreviated.**
  - **(U) UNCLASSIFIED**
  - **(C) CONFIDENTIAL**
  - **(S) SECRET**
  - **(TS) TOP SECRET**



SECRET

OFFICE OF THE SECRETARY OF DEFENSE WASHNGTON ,DC

date

MEMORANDUM FOR DASD (I&S)

SUBJECT: Classification Markings (U)

1. (U) This is an example of a document that contains originally classified information. Standard markings are required for all documents as shown here. These markings include:

a. (U) Portion marking(s) for each section of a document to reflect the classification of the information. When using subsections such as shown here, individual markings are used. When subsections are not marked, the information is protected at the level of protection shown by the overall section.

b. (U) **Overall** markings must be **CONSPICUOUS AND LARGE/BOLD.**

c. (U) A "Classified by" line that includes the name or personal identifier and Position Of the originator.

d. (S) A reason for classification MUST BE USED.

e. (U) A "Declassify on" line that indicates the following:

(1) The date or event for declassification not to exceed 10 years.
(2) The date that is 10 years from the date of the original decision.
(3) An extension beyond the initial 10 years of classification.
(4) An authorized and applicable exemption category(ies).

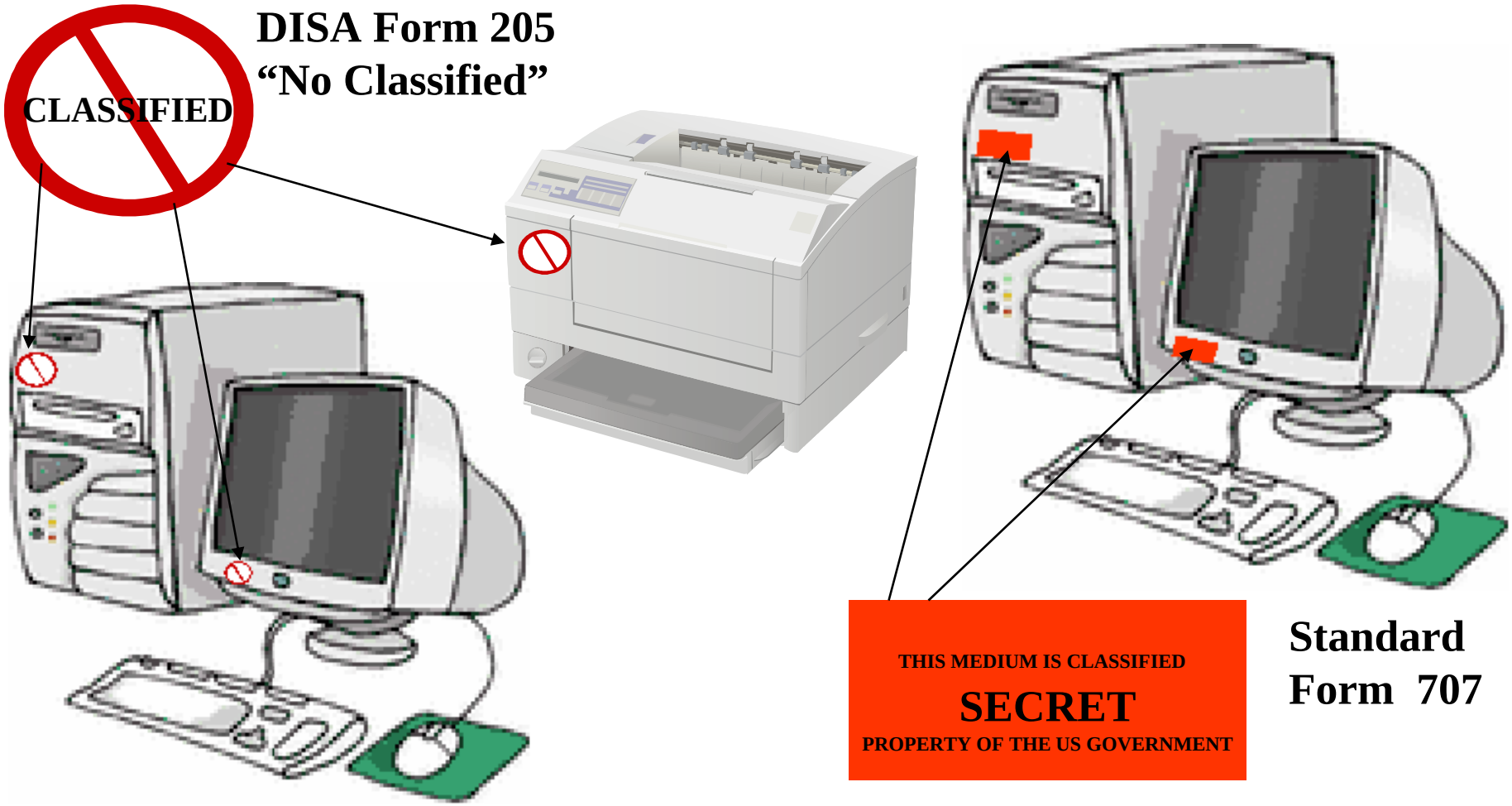
2. (S) If this paragraph contained "Secret" information, the portion would be marked with the designation "S" in parentheses. If the paragraph contained "Confidential" information, the portion would be marked with the designation "C" in parentheses.

Classified by : Emmett Paige, Jr .
ASD(C31)
Reason: 1.5 (a) and (d) *
Declassify on: December 31, xxxx **

SECRET

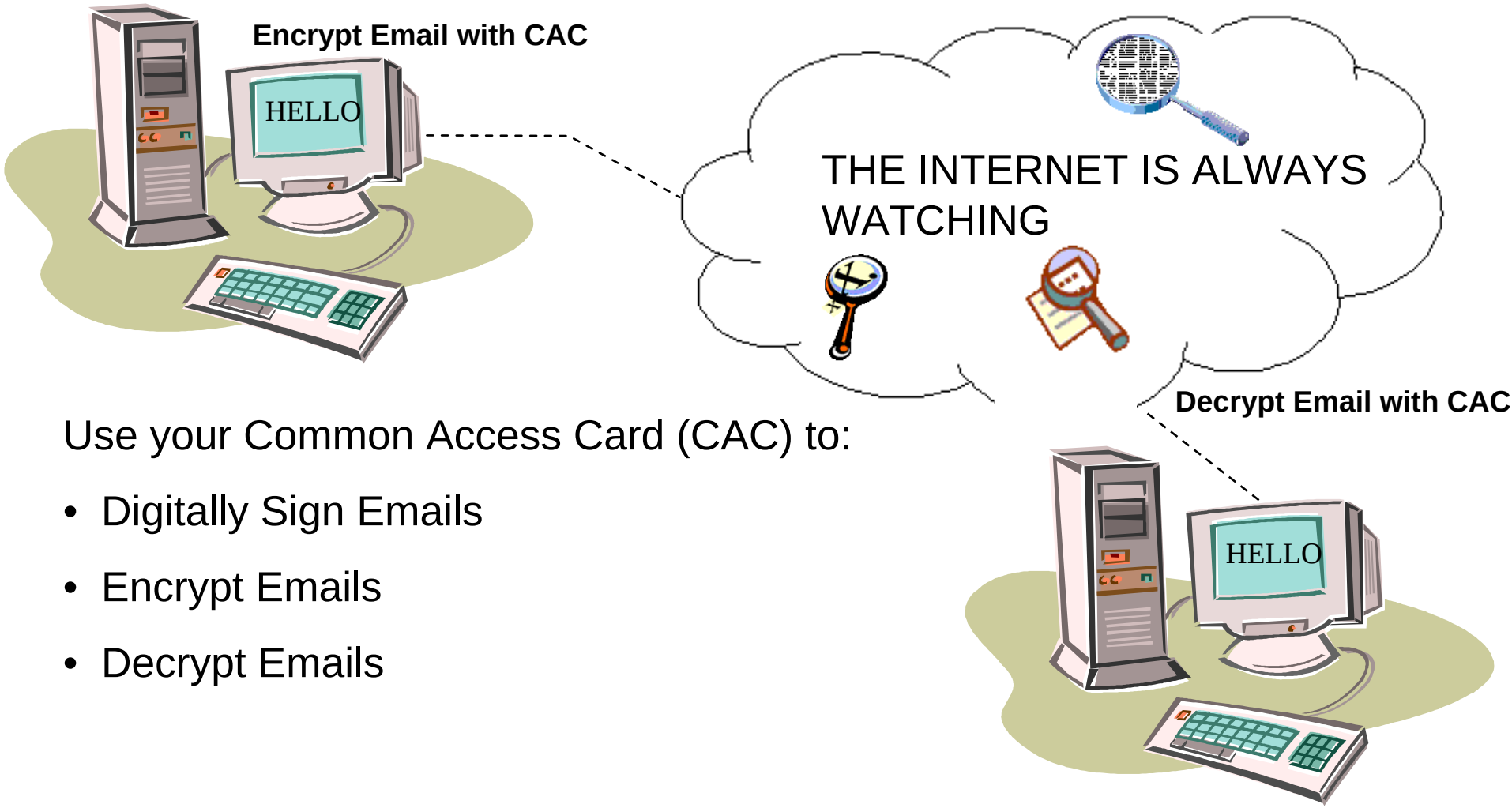
- **Sample of paragraph marking[23]**

Marking Your IT Equipment



Keep ALL labels in clearly identifiable locations.

Information in Transit



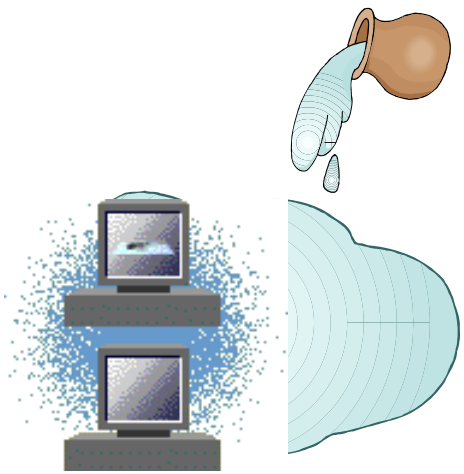
Use your Common Access Card (CAC) to:

- Digitally Sign Emails
- Encrypt Emails
- Decrypt Emails

Sign and Encrypt ALL sensitive DOD information!

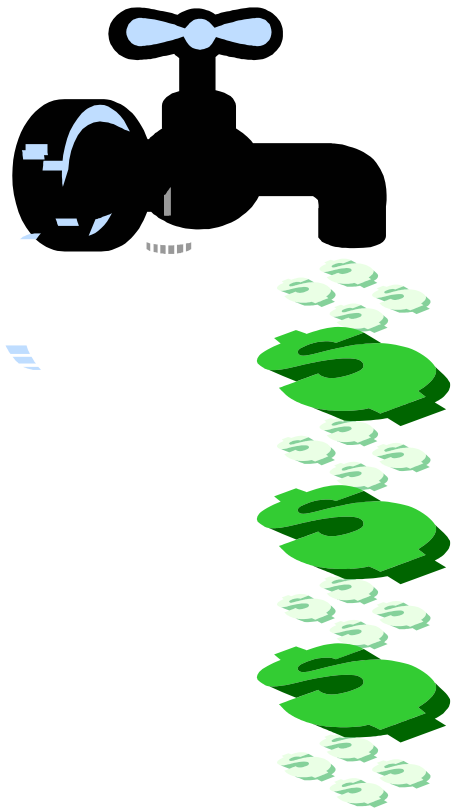
What's a Spillage?

- **It is a form of System Contamination.**
- **It is the Improper storage, transmission or processing of CLASSIFIED information on an UNCLASSIFIED system or via a communications path.**
  - **Most common occurrence is transmission via email.**



Why is Spillage a 'Hot Topic?'

- Can result in denial of service.
- Handled incorrectly – can result in costly mistakes.
- Agency numbers:
  - FY 2002: 27
  - FY 2003: 21
  - FY 2004: 25 (as of 2 Sep 04)
- Resource intensive.
  - It takes 3 weeks to close a spillage.
- Impacts the security of DOD missions.



Cost of Recovery: 1 Incident

Time Spent Researching Compromise	16 hours	$ 418.40
20 Mailboxes Involved; 15 minutes to Clear Each	5 hours	$ 130.75
Scrub Operations (first server only)	7 hours	$ 366.10
Additional Servers Scrubbed	6 hours	$ 156.90*
Daily Backups Lost	3	$1800.00**
Additional Hours	19 hours	$ 496.85***
TOTAL		$3369.00

* Add .5 hours for each additional server

** Tapes cost $65-$85 each (estimate 8 tapes per day)

***Trouble Shooting/Additional Measures

Activities responsible for incidents will PAY for the cleanup!

Why is This Happening?

- Users are not reading Email completely.
- Electronic media is not being marked properly.
- File names or subject headers do not reveal content sensitivity of information.
- Rules for “data aggregation”/derivatively classifying are not well understood.
- Individuals are unaware of classification guides/guidance.
- Improper storage, transmission, processing of classified information.
- All DISA personnel are PERSONALLY responsible for protecting sensitive and classified information.

Bottom Line: THESE INCIDENTS MUST STOP!

Processing Classified Information

- Workstation allowed to process classified information if:
  - In approved open storage area.
  - Contains removable hard disk in unsecured area.
  - Not connected to unclassified Local Area Network/Wide Area Network.
    - e.g., DISANet
- Ensure access is controlled.
  - use approved passwords and change periodically.
- Never transfer information from a classified to an unclassified system without authorization from the Chief Information Officer.
- Never use personally owned computers to process classified information.

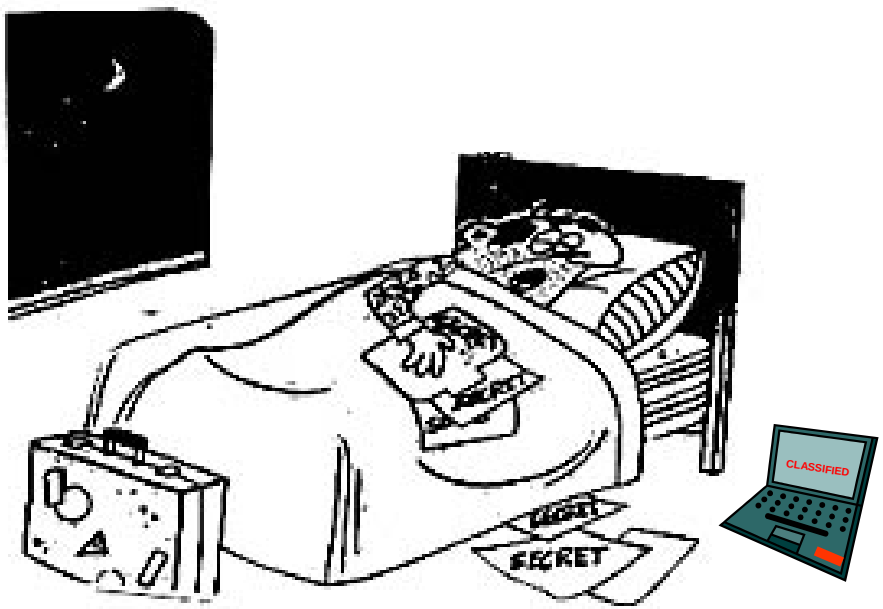
Connecting to a CLASSIFIED Network

- **Workstation must have a removable hard drive**
  - **This requirement can be waived if there is a proof of "Open Storage"**
- **Monitors must face away from any opening**
  - **If this can not be accomplished, an *approved* privacy screen must be used**
- **All doors and windows near CLASSIFIED assets must be covered**
- **CLASSIFIED CPU's should be at least 3 feet from UNCLASSIFIED CPU's**

Keep CLASSIFIED information from other's view!

NEVER Take CLASSIFIED Material Home

- **If you do, you could:**
  - **Be subjected to an espionage investigation.**
  - **Lose your access or security clearance.**
  - **Lose your job.**
  - **Be prosecuted pursuant to statute(s).**



Safeguarding - When Not in Secure Storage

- Keep CLASSIFIED material in your possession at all times until it is either passed to a trusted person or stored in an approved storage container.

- You must be an approved courier when transporting CLASSIFIED material outside of your building.
  - Ensure material is double-wrapped before leaving building.
- All documents must be properly marked and protected by cover sheets.
- NEVER leave classified information unattended.

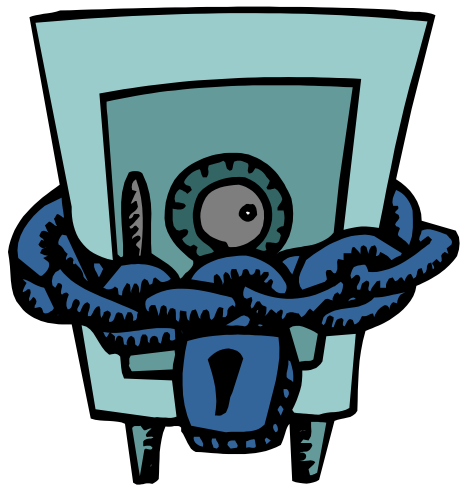
- NEVER discuss classified information on non-secure telephones.
- NEVER discuss, read, or work with classified information in public places.

Security Containers

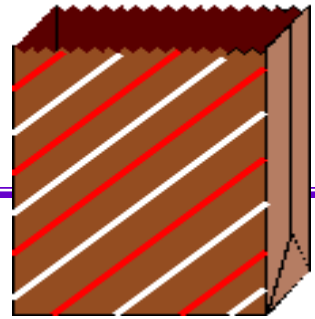
- **Store and protect classified information in GSA-*approved* safes.**

- **Memorize combinations: they are classified and cannot be written down or carried on your person.**

- **SF 700, “Security Container Information” records emergency contact information of all individuals having access to safe.**



Destruction



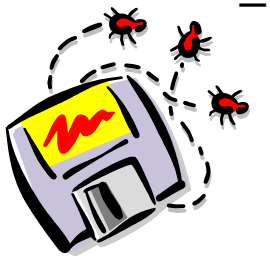
- **Dispose all classified paper, diskettes, and other classified waste in “burn bags.”**
- **Cross-cut shredding also authorized method of destruction – must be on NSA list of *approved* shredders.**
- **TS requires destruction certificates.**
- **Send Hard Drives to N**

Attn: CMC – degaussing
Suite 36875
9800 Savage Rd.
Ft George Meade, MD 20755

Reporting Computer Security Incidents

Security Incident

- **An attempt to exploit a national security system; may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or denial of service.**
  - **Security incidents include:**
    - **penetration of computer systems**
    - **exploitation of vulnerabilities**
    - **introduction of computer viruses or other forms of malicious code.**



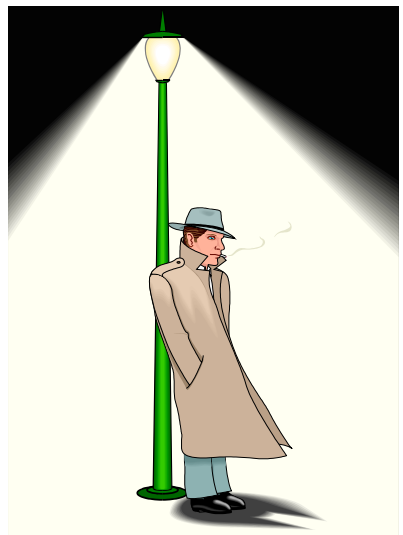
If an incident occurs:

- **Gather all pertinent information.**
  - **time, details, person(s) involved, actions taken, etc.**
- **Report it to the computer help desk.**
- **Site administrators should notify NetDefense [DOD-CERT].**
- **If a violation of law is evident or suspected, the incident must also be reported to both security and law enforcement organizations for appropriate action.**

Report ALL Suspicious Activity!!

Reporting Suspicious Activities

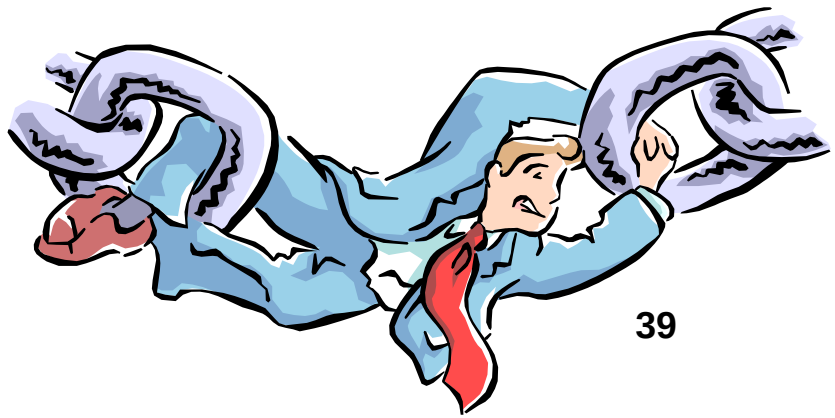
- **Report suspicious persons or circumstances immediately to your supervisor, Facility Security Manager or the Security Division (MPS6).**
- **Be alert for:**
  - **surveillance attempts.**
  - **suspicious persons or activities.**
  - **individuals using unauthorized recording devices.**



Let's Review

To Improve our Security Program

- **Be a strong link in the security chain!**
- **Keep passwords safe! Adhere to password standards.**
- **Separate government work from personal activities.**
- **Working from home? Scan your removable media for viruses when you come back to the office (if you are using your home computer). Keep your government work on government-provided media – don't leave it on your home hard drive.**
- **Watch what you upload and download from the INTERNET or where you 'travel' on the WEB...your computer activity is subject to monitoring.**
- **Adhere to DISA email standards.**



To Improve our Security Program (cont.)

- Separate classified from unclassified information. Use classification guidance when regrading classified information. Label your diskettes!
- Keep track of your removable media. Store them when not in use.
- Watch your file transmissions! Make sure the files you transfer or the email you send is appropriate for the sensitivity of that network!
- Turn on your screensavers and activate password protection. Keep your files and access to the network safe!
- Report anomalies. Requests for information from unknown sources (foreign countries), destroyed, infected or corrupted files, missing computer hardware, etc. Report this to your Information Assurance Manager and to the Help Desk.
- Traveling with a government computer? Keep track of it!

Conclusion

- **<u>Strictly</u> follow DOD and DISA security guidance. If you don't know - ask!**
- **Contact your Security Manager, Information Assurance Manager (IAM), or the Security Division (MP6) for assistance.**
- **Pay Attention to Detail.**
- **Be Alert.**
- **Be Aware!**

Security is your responsibility!

We're Almost Done!

Do you want credit?

I certify that I have read and understand the material presented in this slideshow.

I acknowledge that I am responsible for knowing and following the information presented in this guide.

Click here, sign in for credit and print your completion certificate.

(Special note: the certificate link is only intended for DISA customers. Certificates will NOT be issued for non DISA customers.)

Press the Esc key on your keyboard to exit Slideshow.


DEFENSE INFORMATION SYSTEMS AGENCY